Defining Cyberspace as a United States Air Force Mission

GRADUATE RESEARCH PROJECT

Pamela L. Woolley, Major, USAF
AFIT/IC4/ENG/06-09

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this graduate research project are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/IC4/ENG/09-09

Defining Cyberspace as a United States Air Force Mission

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of C4I Systems

Pamela L. Woolley

Major, USAF

June 2006

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/IC4/ENG/06-09

Defining Cyberspace as a United States Air Force Mission

Pamela L. Woolley, BS, MA

Major, USAF

Approved:

_____	_____
Robert F. Mills, PhD, USAF (Chairman)	date
_____	_____
Richard A. Raines, PhD, USAF (Member)	date

Abstract

The purpose of this research was to provide a common framework and language for the definition of cyberspace. Specifically this project looked into three key areas what cyberspace is, why it is unique and important, and the capabilities and mission areas. An extensive literature review was completed. The research indicated that the fundamental problem of defining cyberspace evolved as cyberspace evolved within each community in the Air Force.

The culmination of this effect was an encompassing definition as well as a set of models to graphically depict cyberspace and the interactions with the other information domains.

Acknowledgments

I would like to express my sincere appreciation to my faculty advisor, Dr. Robert Mills, for his guidance and support throughout this effort. His insight and experiences in the technical and academic communities were invaluable and greatly appreciated.

I would like to thank Major Kristina Roth whose insight helped build the foundation though our many projects together. Finally, I would like to thank Major Aaron Dyke who provided me support and perspective to bring this project to fruition.

Pamela L. Woolley

Table of Contents

List of Figures

Defining Cyberspace as a United States Air Force Mission

I. Introduction

Background

Everyday we are becoming more reliant on this thing we call "cyberspace." In February 2003, the National Strategy to Secure Cyberspace was released outlining the importance of cyberspace. On December 7, 2005 the Air Force (AF) Chief of Staff released the following new mission statement for the AF "*The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests—to fly and fight in the Air, Space, and Cyberspace."* The addition of "Cyberspace" to the mission statement let many to ask, what is cyberspace? And what does it mean to have Cyberspace as a mission area?

Unfortunately we all use systems within cyberspace and to some degree we all have our own definitions of what it is, and that IS part of the problem. When asked what the Air Force means to have "cyberspace" as a mission statement, nearly every time the first question that comes up is "How do you define it?" Before the AF can effectively organize, train and equip the forces to take on the mission it fundamentally has to agree on a common language to describe cyberspace. This is a very complex issue, with many stakeholders within the AF talking about the pertinent issues, but using different terminology that has evolved in response to their particular organizational experiences.

We have to get back to basics, establish a fundamental framework describing cyberspace, why it is important, and our capabilities in cyberspace.

Research Impact

When the AF added Cyberspace to the mission statement, this caused a lot of uproar about what cyberspace is and how it is defined. AF personnel understand Air and Space, but cyberspace is different because it is still evolving. This research aimed to develop a definition and a model of cyberspace to form a foundation for organizing, training and equipping the force to defend and exploiting cyberspace as a mission area.

II. What is *Cyber* space?

Definitions

One satisfying, encompassing definition for cyberspace does not exist and that, in some cases, existing definitions contradicted each other. As defined by the University of New Orleans, cyberspace is "The non-physical space where interaction takes place between computer networks." (University of New Orleans, 2006) Another definition seemed much more simplistic: "the electronic medium of computer networks, in which online communication takes place." (Dictionary.com, 2006) Princeton University defines cyberspace as "a computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange" (Princeton, 2006). Finally, Joint Doctrine defines cyberspace as "The notional

environment in which digitized information is communicated over computer networks" (JP 2-01.3, 2000, p. GL-4).

Overall, most definitions include some reference to computer networks, either virtual or actual. Some include reference to the information space and resources, while others include the services or resources available on the internet, and some discuss geographic dislocation. There is agreement on the origin of the word: cyberspace was originally coined by William Gibson in his 1984 novel Neuromancer (University of Arizona, 2006).

Not only do these definitions contradict each other, these definitions do not clearly capture what cyberspace really is. Irrespective of if they agree that it is a real thing, there is agreement that cyberspace is a boundless environment that is deeply integrated into many aspects of our daily lives in America as well as many other countries around the globe. Cyberspace extends even beyond this planet. Systems like the Hubble Space Telescope, the Mars rovers, Sprit and Opportunity, and the Global Positioning System pass information through cyberspace from orbit and beyond.

All of the above definitions provide some insight, but a standardized, encompassing definition needs to be established that can be effectively utilized by the disparate users of cyberspace. To accomplish this task, this paper will work to define the existence of cyberspace, delineate its boundaries, if possible, articulate the impacts that cyberspace has on both military and civilian processes, and then relate this definition to capabilities that can be coordinated within the Air Force.

Does cyberspace exist? It is definable at some level because of all the physical components that create cyberspace can be seen and touched. The information passing on

the lines between this computer and the rest of the world may be difficult to comprehend, but it is transferring information across something. Additionally, interfaces with the physical world (i.e. a person to person conversation in the same room) and are not using it. Furthermore, places can be identified that "have" global connectivity and the ones that do not. For example, in some remote areas of the world (such as deep in the mountains or unpopulated islands in the middle of the ocean) if you do not have a computer or an access point to a telephone or computer network that can transport data, then you probably cannot access it. It must exist. Furthermore, *cyberspace* did not exist 200 years ago. It is a space that was created by humans in order to store and move information from one person to another. It did not exist before we started building things that would send electrical signals down wires (i.e. the telegraph, the telephone or the computer network) or through the air (i.e. wireless telephones and networks).

So if it exists, can boundaries be identified around it? The size of and the knowledge contained within cyberspace grows every time a new computer is plugged into the internet, some new information is made available through some network or an entirely new network technology is born. However, a boundary may be defined based on how the information is stored. While the initial purpose of cyberspace may have been to simply move information, when digital technology was born giving rise to the computer, we began to store vast amounts information as well. The processing and storage capacity of the computer is truly what gave rise to cyberspace as we know it today. Therefore we can define one type of boundary around cyberspace, as the *digital* environment.

The most appropriate definition of digital is defined as "of, relating to, or using calculation by numerical methods or by discrete units" (Merriam, 2006). Today, in the

case of the computer, ones and zeros are used to define the digital environment. However, we should not consider it the *binary* digital world because that will limit the definition to what we have today instead if other possible forms of digitization (i.e. quantum computing) that may be in our future.

Cyberspace uses analog waveforms to transmit data between computers; however it is transformed back into a digital format when used on either end of the link. These links are critical however, without the digitization cyberspace would not have the power and capabilities that is does.

Digital information can be easily accessed, copied and stored with much greater accuracy than analog signals could be (Negroponte, 1995). Do you remember finding the beginning of your favorite song on a cassette tape? Compare that to how we search for specific songs on the Compact Disc (CD) or on our computers. The signals were stored using analog technology on the cassette tape but it is stored digitally on the CD and computer systems making it much easier to find. The life span of your digital music is significantly longer as well. As long as your CD keeps working, your music will never wear out like it did on a tape. Additionally, you can make as many copies as you want and the signal will not get degraded like it did on the tape. You can even listen to digital media with a variety of different equipment such as an MP3 player, car stereo, directly from your hard drive, or even on your telephone! Cassette tapes required the use of a cassette tape player in order to hear the music. Digital technology enabled cyberspace, which enabled the creation of the internet, however cyberspace is clearly larger than just the internet. The internet is only one system of many systems that reside in cyberspace. Some systems utilize cyberspace without actually being connected directly to the internet,

for example digital telephone networks and automated teller machines (although some of these are evolving to use the internet).

If cyberspace exists and can be defined as the *digital* environment, does this capture the true essence of what it is? Outlining what it does will enrich the definition. Fundamentally, the only four basic reasons we use cyberspace today is to collect, store, process and transmit information. The desired effects may be communicating with a friend, posting pictures to a website, or writing the next best seller, but fundamentally it is all about information. If we remove the "intent" we are using the systems within cyberspace to collect, store, process and transmit information. That is why it is often referred to as the "information space."

Collecting what we have so far, we could say cyberspace *is the human created electronic digital environment used to collect, store and transmit information between electronic equipment*. However, limiting the definition in this manner is analogous to limiting the definition of water to hydrogen and oxygen molecules or "Airspace" to "the space lying above the earth or above a certain area of land or water" (Merriam, 2006). In order to fully appreciate what it is, additional context needs to be added to fully explain the essence of cyberspace.

Searching for parallels in the air and space doctrine yielded some interesting conclusions. Neither "air space" nor "air and space" is defined in joint or Air Force doctrine. While Air Force doctrine may not specifically define "air and space" it does define many air and space components, for example *air and space power* is defined as "the synergistic application of air, space, and information systems to project global strategic military power" (AFDD 1, 2001, p. 94). The closest definition to "air space"

and/or “air and space” is *aerospace*. The basic definition according to Merriam Webster is “space comprising the earth's atmosphere and the space beyond” (Merriam, 2006). In Joint Doctrine this was modified to include context so it is defined as “Of, or pertaining to, Earth’s envelope of atmosphere and the space above it; two separate entities considered as a single realm for activity in launching, guidance, and control of vehicles that will travel in both entities” (JP 1-02, 2001, p. 9). The definition in joint doctrine has been enriched with the activities conducted in that particular space; in this case, the activities described are launching and control of vehicles within air and space.

Applying this same thinking, we need at add the context of what military activities are conducted in cyberspace the above definition. Unfortunately, unlike aerospace, we use cyberspace for everything so it is deeply integrated into almost every process that we have. Through the few short years since this digital environment went mainstream, it has infiltrated our lives at nearly every level to the degree that it changed our entire culture! For example, AF members no longer receive their pay check or even their Leave and Earning Statement in the mail, all the information is moved through cyberspace. Cyberspace is not limited by organizational, cultural, political or national borders. As technology evolves, processes evolve away from the traditional ways of doing things and become dependent on cyberspace. As a result of our dependence on cyberspace and because it is so interconnected with many processes, the National Strategy to Secure Cyberspace defines cyberspace as “the nervous system of [our critical] infrastructures—the control system of our country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables

that make our critical infrastructures work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security" (White House, 2003, p.16).

Putting this all together, I submit the following more comprehensive definition: Cyberspace is the human created digital medium used to collect, store and transmit data and information between electronic equipment enabling nearly instant, boundless, global connectivity without respect to organizational, cultural, national or political borders. This medium is the nervous system of our critical processes and infrastructures, essential to the health of our society. Finally, the level of interconnectivity, the accuracy and fullness of content, and availability characterize cyberspace and its ultimate capabilities.

Models

Models are often used to visually represent something that is difficult to see, or as in the case of cyberspace, impossible to see. All models have their limitations, but overall normally provide a great way to describe difficult concepts. There are many models that attempt to represent cyberspace. Unfortunately many of these are very technology and component (i.e. computer network) focused. However, there are models that might be adapted for cyberspace.

Many of the models I reviewed separated the domains into three distinct domains physical, cognitive, and information, although the representations differed. For example, Figure 1 shows the three domains as overlapping circles with Network Centric Warfare (NCW) in the middle.

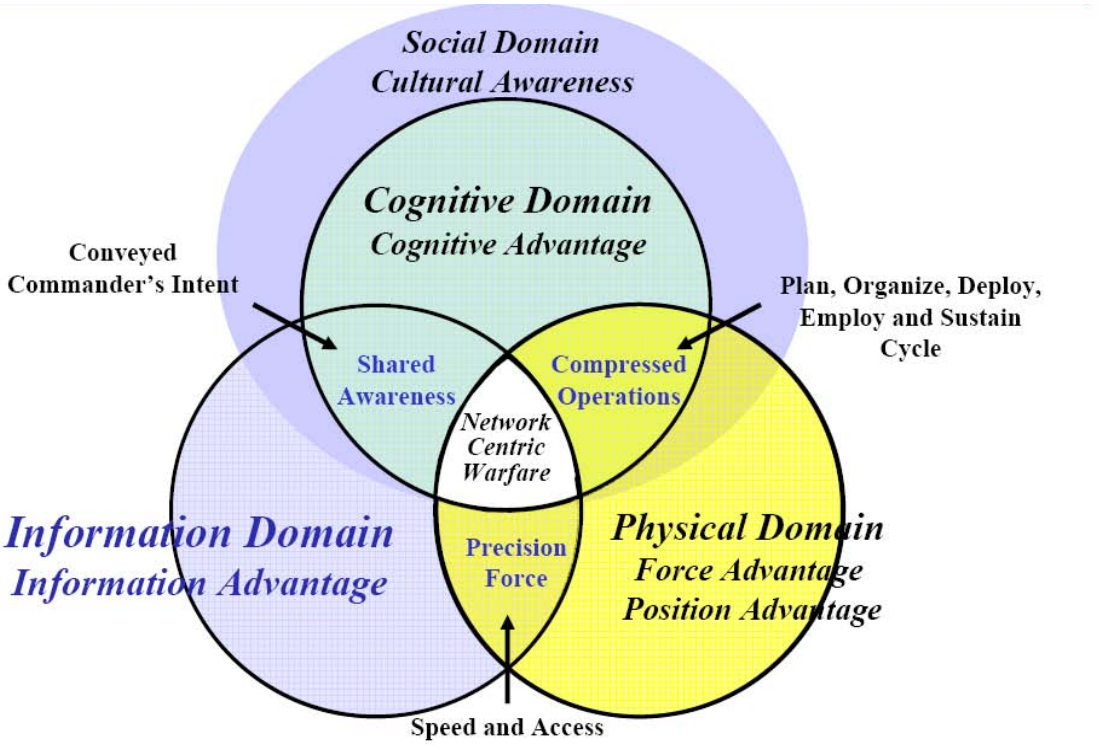

Figure 1. NCW Domains[1]

This model has a significant value; however this model seems to imply that the information is bounded. Implying that the only information in the physical and cognitive domains is where the circles overlap. It would be adequate to use as a model for cyberspace because it can not clearly represent that information is everywhere.

The next model, Figure 2, again showed three domains of information but with the cognitive and physical domains separated by the information domain.

[1] Source: Alberts, 2004

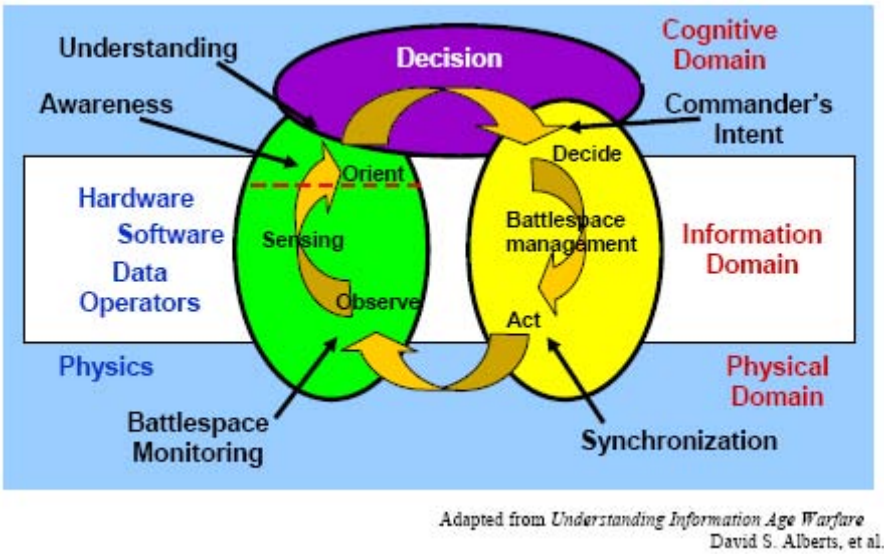

Figure 2. Another View of Information Domains[2]

The insightful addition to this model is the Observe, Orient, Decide, Act (OODA) model created by John Boyd. This model was adopted for Command and Control (C2) doctrine, and from that perspective may be sufficient. It has the same fundamental domains physical, information and cognitive as the first model, and cyberspace is not easily depicted. Most models in the literature include these 3 domains in some form; so they are the basis for the new model in Figure 3. Information is everywhere in some form, it is not confined to a particular domain and eliminated in others domains. This is critical because, as mentioned before, the reason cyberspace exists is to handle this information.

Interestingly, most people have difficulty describing "the information space." I believe this is at least partly a problem of perspective. Dr. Alan Heminger, Associate Professor of Information Resource Management at the Air Force Institute of Technology, shared a great example of how our perspective of information changes our description of

[2] Source: AFDD 2-5, 2005, p. 3

it. Imagine a small glass fishbowl like one you would purchase at the local pet store. Fill it with water and add a goldfish. Now, ask yourself, "what is water?" It is easy for us to identify because it has been bounded by the bowl. But change your perspective and ask the gold fish to identify "what is water" and it will have a more difficult time, because for him/her water is everywhere and everything. It is the thing that keeps it suspended, it provides the environment to make its propulsion system function, it is the place where he/she finds food and oxygen, and most importantly he/she would die without it. Information is like the water in the bowl for us. It is everywhere involved with everything we do, and we could not survive without it.

In the following model, the basis of the model is that information is everywhere instead of bound to just one circle adjacent to the physical or cognitive domain, instead it is in both.

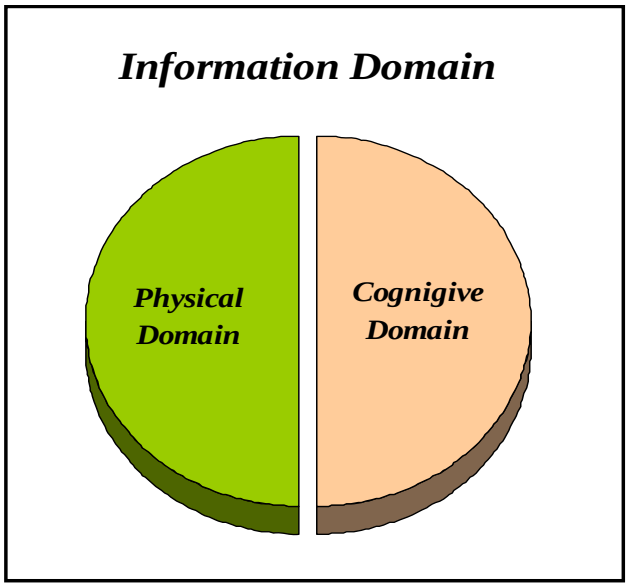

Figure 3. Information Space

The physical domain is the information about the physical world where we live. It is how things *actually are*. The cognitive domain is how we *perceive* the information. This is the information in people's minds about aspects of our environment. There are many complex interconnections between the information in the cognitive domain, but it may be an incomplete representation of the information. For example, if I show you a building, you may be able to describe what it is made of, approximately how tall it is, and the color. There are aspects of the building you may not know such as the temperature or how many rooms it has in it. This information resides in the physical world, but we do not *know* it because we have not absorbed it into our cognitive domain.

So where does cyberspace fit in? Back to the fundamental definition, cyberspace is a human created digital medium in which we collect, store, and transport information. There are instances where it simply collects information from the physical world, such as through capturing imagery. Additionally, we can enter the information from our cognitive domain into cyberspace. Either way it gets there, once the information is digitized in cyberspace it can be stored. Adapting the diagrams above, I submit that cyberspace is the third dimension of information as shown on the following graph:

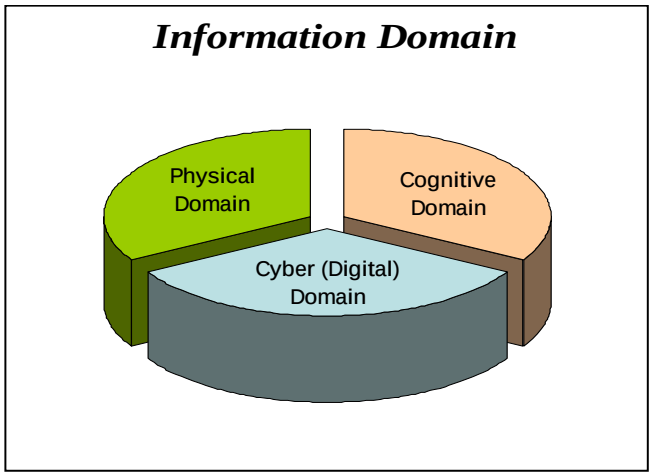

Figure 4. Cyberspace

The information in cyberspace is how information from both the physical and cognitive perspectives is *represented.* This is the digital domain of information. Acknowledging that all models have their limitations, there is obviously part of the cognitive domain that is obviously physical (i.e. the physical grey matter of the brain) and there is obviously an aspect of cyberspace that is physical (i.e. the actual computer, routers and switches and the wires that connect them). As an analogy, think of the actual physical components of the different domains as the *crust* of the pie and the information attributes are the *custard* contained within that pie. In the physical domain, the *crust* are the items such as the actual physical table, the *custard* are the information attributes such as the color of the table, the height, the temperature. In the cognitive domain, the *crust* is the grey matter the physical brain, whereas the *custard* is the thoughts and the mind. So in cyberspace, the *crust* is made up of the routers, switches and computers; the *custard* is the information passing through them. This model is attempting to represent the only the custard, and show that information exists everywhere. Information can exist simultaneously in different domains. However, based

on the actual physical attributes, how we perceive it, and how we represent the information may vary slightly which presents a minor limitation in how we record information in cyberspace. How we record the height of the building may not capture all of the information. If the building is 30 ft high and we inaccurately record it has 300 ft high, it does not change the physical information of the building or how we perceive it, unless we perceive it through cyberspace instead the physical world. Additionally, recording the height as a number into a database will record significantly different information than if we take a digital picture of the same building and put that in a database. Again, the physical information about the building has not changed, it remains the same height.

Cyberspace interfaces with both the cognitive information space as well as the physical information space as show in Figure 5.

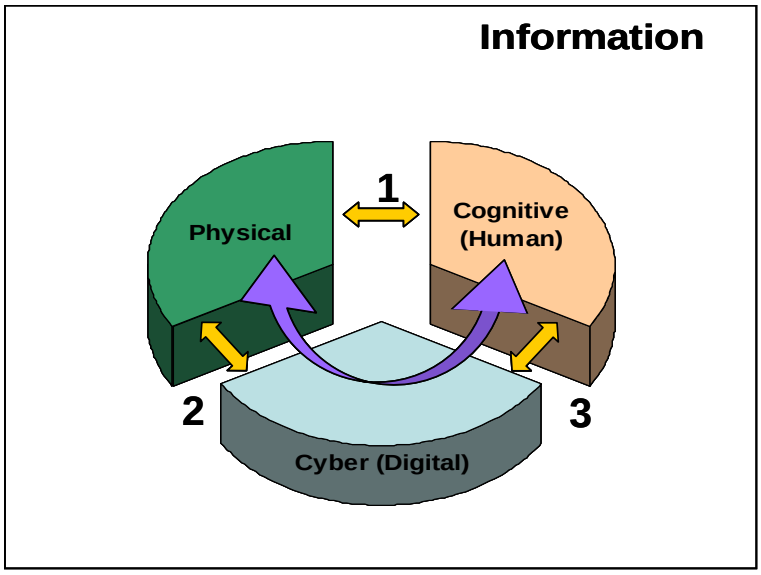

Figure 5. Information Space Interactions

The orange lines represent direct interfaces between the environments. The arrow between the physical and cognitive domains (line 1) represents human interactions with

the physical environment. Examples of this line include human contact, human conversations and directly observing/changing the environment. The interface between the physical domain and cyberspace are similar, an example might be reconnaissance photographs or automated assembly lines that are computer controlled. The interactions between the cyberspace and cognitive domains include entering something into a computer, reading an email from the computer, etc.

The purple lines indicate actions that are through cyberspace in real time. These actions require the electronic link between the humans and another part of the physical world; for example flying an unmanned aerial vehicle (UAV). The human is controlling a distant aspect of the physical world through the interconnected computer systems of cyberspace.

III. Why is Cyberspace so unique and important?

Cyberspace is the medium that we use to collect, store, process and transmit large amounts of information, so its value should be measured not only on the cost of the components that create it, but by the value of the information that is within. To further understand this, we have to understand a little more about information in cyberspace, information through cyberspace and cyberspace's impact on processes/value stream.

Information in Cyberspace

In the book "The Third Wave" by Alvin Toffler, he believes that we are entering the third wave of transformation, the information or knowledge age where our outputs

will be information instead of the agriculture and machines of our past. According to Peter Drucker, "Knowledge is the only meaningful resource today. The traditional "factors of production" - land (i.e., Natural resources), labor and capital- have not disappeared, but they have become secondary" (Drucker, 1994, p. 42).

As we enter this next generation of human development, we need to re-evaluate what our "products" will be. What is the "product" or "output" of America? Corn? Wheat? Semi-Conductors? Steel? Movies? Software? Science? *Intellectual property* is the number one product and export in America. In the entertainment business alone, movies (both ticket sales and DVDs) have already exceeded the overall sales of steel (Stone, 2004).

So what is intellectual property (IP)? According to the Merriam-Webster Online dictionary:

- Intellectual is: "of or relating to the intellect or its use; developed or chiefly guided by the intellect rather than by emotion or experience"
- Property is: "**a:** something owned or possessed; *specifically* **:** a piece of real estate **b :** the exclusive right to possess, enjoy, and dispose of a thing **:** OWNERSHIP **c :** something to which a person or business has a legal title **d :** one (as a performer) under contract whose work is especially valuable"

In other words, IP is the knowledge that we use to create something such as a movie, document a new scientific development, a book or even a military operations plan. IP is unlike any other type of property because it can be shared without losing value. Unlike physical goods, IP it is not consumed as it is used. Contrary to material wealth, sharing knowledge actually increases its value (Zack, 1999, p. 129). For

example, an invention or movie/song that is never codified in some shareable medium will never be worth any monetary value, whereas if it is shared many copies can be sold. Even in the cases such as trade secrets, sharing that knowledge would also increase its value, but for someone else if it was stolen.

In the commercial sector of American society as we outsource more and more of our industrial products, we need to ensure we are compensated for our informational products. In the military we need to continue to be vigilant to keep our IP safe from compromise. Increasingly this information is stored in the digital domain of cyberspace. This is the information that resides on personal computers and servers around the world. It can be easily shared and, more importantly, unlike a book, it never goes out of print so it may be perpetually accessible (Negroponte, 1995).

This evolution, this rising importance of intellectual property, has caused drastic changes in our military and our national economy. "Knowledge has become *the* resource, rather than *a* resource. It is what makes our society "post-capitalist." This fact changes – fundamentally- the structure of society. It creates new social and economic dynamics. It creates new politics" (Drucker, 1994, p. 45). Unfortunately, the laws that govern and protect this type of information are far behind the technology. Additionally, because cyberspace does not recognize national borders, it becomes a significantly more complex issue. Even if we were able to establish and enforce laws in the United States, we would still continue to be vulnerable to those outside the United States. There are many opponents to this type of control. Those who oppose IP law feel that all information should be free and we all have a right to benefit from our collective genius. The *Pirates of Encryption* state "anything they can get their hands on is legally theirs"

(Halbert, 2005, p. 11) even if they have to employ hacking methods to get to the information. To them, IP laws simply impedes the free trade of information and knowledge, resulting in a power divide controlled by a chosen few, protected by the complexity of IP law. This power divide creates tension in cyberspace, giving some people justification to become hackers. Our adversaries are no longer from the nation states of the past; they could (and do) come from within our own national borders.

Information through Cyberspace

Initially, the idea of information moving through cyberspace as a separate idea may seem redundant. However, the information that is described in this realm is not the traditional information stores of the past but the information that transverses cyberspace with one mission, to build an interface and directly interact with the physical world in real time. Cyberspace has dramatically changed how we interact with the physical world, causing a renewed growth in concern about security in cyberspace. This growing concern over what can happen in the physical world through cyberspace was a key catalyst for writing the 2003 National Strategy to Secure Cyberspace. Innovation creates more systems that directly impact cyberspace everyday such as manufacturing systems, banking and stock market systems, supervisor controlled data acquisition (SCADA) systems and military systems like UAVs. These systems have the potential to no longer just disrupt our operations; they have the power greatly enhance people's lives or literally take them.

First, computer modeling and simulation are getting so advanced that we can now manufacture complex objects of our raw materials at the click of a button. For example

getting a porcelain cap for a damaged tooth has significantly changed. In the past if a patient were to go in for such a procedure, the dentist would make a mold of the patient's tooth, send the mold and the instructions to a lab to have the new porcelain cap created. After about a week to ten days, the patient would return to the office and have the temporary cap removed and the permanent one installed. Today a patient can actually go to the dentist office to get a porcelain cap for your teeth and never leave the dentist chair. Modern technology has evolved to the point that the dentist can do a three dimensional "scan" of the tooth in question into a computer system, create the porcelain cap, and "print" the tooth out and install it, all in less than 2 hours without the patient leaving the office. This example clearly illustrates how computer modeling, simulation and creation have evolved to the point that we can literally replicate physical objects at will. The applications for this may be endless. A great military application may be rapidly reducing the supply chain, we can just send in the raw materials, and create specifically whatever we need at the destination exactly when we need it. From a science fiction perspective, we still have not evolved to the point of being able to give the Joint Forces Commander a "cup of Earl Grey Tea, hot" like Captain Picard in Star Trek, but we evolved far enough to be able replicate the cup for him/her on demand.

Secondly, the banking and financial industry, to include the security industry, has relied on computer systems that leverage cyberspace connectivity for years. Some examples of this were the automated teller machine (ATM) and telephone banking. While the information they control is predominately numbers and account transactions it can have an impact, although *normally* not devastating, if they malfunction. If the connection is lost between the ATM and the bank, a person may not be able to withdraw

money. While this may seem like a trivial inconvenience it can quickly become a larger problem. For example, in the case of a large scale disaster like Hurricane Katrina where people were not able to access their money or use credit cards, they were could not purchase goods (such as gas, food and water) and services (such as hotel or transportation) so it literally stranded thousands of people in the most devastated areas of the gulf coast and added to the already critical problem of human survival.

However, it is the SCADA systems that are causing the most concern. (White House, 2003, p. viii). SCADA systems are "a computer system for gathering and analyzing real time data" (Webopedia, 2006). These systems monitor and control larger systems that exist beyond the bounds of cyberspace such as electrical transformers, water systems, trains, pipeline pumps, chemical vats, and radars (White House, 2003, p. viii). They are not new systems, in fact they have been used for over 30 years, however as we increase the external network connectivity to these systems we greatly increase the vulnerabilities. These systems can be as simple as monitoring environmental conditions such as temperature or as complex as physically controlling valves and electrical transformers. If these systems were disrupted they could cut power to large populations for a long duration of time. Again, while this may initially seem like an inconvenient problem, it would create a strain on our resources if the entire power grid of New York City were cut during a severe winter storm. More likely, the experts predict that the hackers would simply change the monitored readings so that the human in the loop would actually be the one to take the system off line (instead of the computer), but the effect is the same. (Cyber War!, 2003)

Finally, through the innovation of UAVs we are able to impact the physical environment from great distances. UAVs have become an invaluable source of real time imagery during combat operations in both Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF). But more importantly, these same vehicles have carried weapons that were launched literally from the other side of the world. UAVs are a critical resource because they allow us to take our people out of harms way, but only if we have the connectivity through cyberspace to support the real time operations. While we may have created a way to keep people out of harms way, we have created yet another dependence and vulnerability that can be exploited by the enemy. A denial of service attack may cause the loss of the airborne asset, but if the enemy gains control of the unit then we may have our own bombs dropped on our own friendly forces. Because of the growing impacts in the physical world, securing the systems in cyberspace is more important than ever.

Processes/Value Stream Perspective

The third way cyberspace shows us its power is how it has dramatically affected our processes. Technology is one of the key enablers to Business Process reengineering (BPR) and Lean Thinking because it can enable us to do things differently, fundamentally change (and hopefully improve) our processes or value streams.

While this may not initially seem like something we should discuss in the value of cyberspace, not recognizing the stovepipes within cyberspace and the associated affects

in the process we perform can be the difference between a failed initiative and a successful one.

A recent example of this occurred in Air Force Material Command with their e-Business transformation initiative. They attempted to transform over 20 processes ripe for automation; one in particular was the Deployment Readiness Service (DRS). The basic goal of DRS was to build a tool that Unit Deployment Managers (UDMs) could use to track personnel training and readiness for their unit. The prototype system was developed and lauded by all who initially saw it. Unfortunately, it ran into difficulty and was eventually cancelled. Two main problems plagued this program – lack of a process owner and limitations of legacy systems. No one "owns" the UDMs because it is not actually a career field, although almost every unit across the AF has a requirement to deploy personnel. Because no functional community owns the process, there is not anyone with an end to end process perspective or a champion to fund the system long term. Consequently it never received fully programmed funding and the program was cut when it ran out of initial working capital funds. The second problem sprouted from the existing systems. Multiple legacy systems currently being used to partially track the data in DRS were still mandated because DRS only took over part of the functionality of those systems. DRS did not replace the entire system so the legacy systems could not be eliminated. Additionally, the older legacy systems could not be interfaced with DRS without significant capital investment. Since the systems could not either be turned off or electronically interfaced with DRS, the UDMs had to maintain two sets of data, which in the end would have added workload instead of eliminating it. In the end the effort was cancelled after the AF had obligated over $50 million in funding alone. (Heminger and

others, 2006) The AF communities need to start working together to break these stovepipes down when building new systems instead of just building better stovepipes. We need to approach this from a BPR/Lean perspective.

In BPR, a process is "a collection of activities that takes one or more kinds of inputs and creates an output that is of value to the customer." (Hammer, 2003, p. 38). The same concept is evident in Lean Thinking known as the value stream. The value stream is created by "identifying every action required to design, order, and make a specific product" (Jones, 2003, p. 37). The two books, *Reengineering the Corporation* and *Lean Thinking*, do use different terminology and make some distinctions on actual implementation but fundamentally are talking about basically the same thing for the purposes of this paper – eliminating unnecessary steps and waste in our processes.

In order to reengineer a process or lean a value stream, you "*fundamentally* rethink and *radically* redesign the processing to get *dramatic* improvements in critical, measures of performance such as cost, quality, service and speed" (Hammer, 2003, p. 35). The organization has to break the stove piped rules, throw away the old process and start over looking at the value of the steps being done to complete the product/service. Instead of focusing on just outputs the focus becomes outcomes.

The systems in cyberspace generally provide a capability that allows us to redesign processes. In order to gain the full value of the new process with the waste removed; we have to be careful to not just automate the process. In order to gain this full value, it has to be tied back to the high level business strategy and ultimate value to the customer. If you reengineer/lean a process too low, you will not be able to get rid of the

waste within an organization because there are many steps and controls in the process that are considered critical because of how the process is currently executed.

For example, when the AF 988 (the leave form) could be filled out using an computerized tool such as Form Flow, this did not "reengineer" or radically improve the process itself. Only one aspect of the process was impacted; filling out the initial form. Overall, the process remained fundamentally the same as depicted in figure 6.

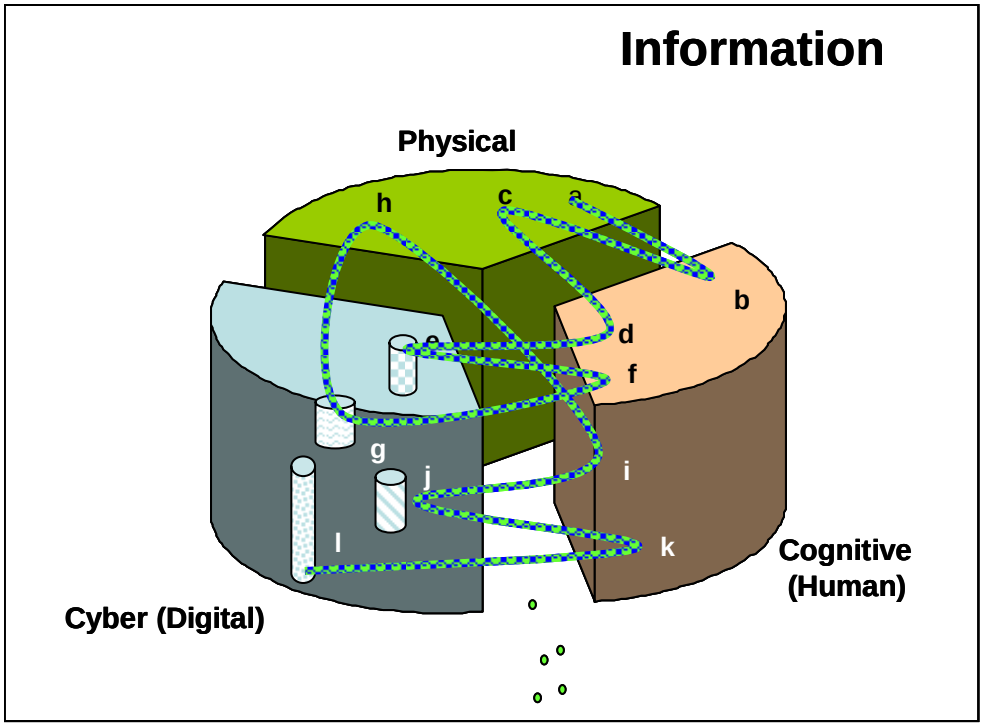

Figure 6. Leave Process Example

a. A friend invites you on vacation
b. You determine if you want to go
c. You talk to your boss to determine if you can have the time away from work
d. Leave is approved, begin paperwork
e. Access the pay system to determine if you have leave
f. Leave amount is sufficient
g. Access the program to process the paperwork (Form Flow/IMT viewer)
h. Print out the information and get your supervisor to sign it
i. Take it to the orderly room
j. They enter the information into a third, non-connected system
k. The information is forwarded to finance

l. The information is then entered into the pay system, a fourth non-connected system

Depending on the reliability of the intra-office mail system and how geographically separated the three sets of people (member, supervisor, and orderly room) were this process could take a significant portion of time out of the day for the member to process the paperwork.

However, when LeaveWeb was created it did reengineer the process because it eliminated non-value added steps in the process as reflected in figure 8. With LeaveWeb, everything can be done without the member leaving his/her workspace, assuming they have a computer with the required network connectivity. Not only did this save hours of time for the member it also increased the overall accuracy of the information. The data accuracy increased because it is only entered once by the member instead of multiple times by multiple people in the process (i.e. the member, the orderly room, and finally finance). This system is now standardized across the Air Force so orderly rooms no longer need to maintain their homegrown systems for tracking because they can utilize the tracking features built into LeaveWeb.

Not only do we need to integrate our information so that it can be shared, we also want to avoid losing information as we traverse the different domains. Every time we cross the divide between the domains, we risk losing information because we may not be able to comprehend or store it accurately. For example, when you take a normal digital photograph of a birthday cake, you lose the smell and taste and to some degree texture of that cake. The same is true of other information databases because there may be critical information that should be stored but there isn't a field for it in a particular application.

Reducing the non value added steps in a process helps to close the gap between the different domains and should reduce the lost information because only the necessary information is kept. The following graphs step through an example:

The small green "dots" of information in figure 6 represent the information that was lost due to traversing the interfaces, for example how many leave forms were not processed through LeaveWeb. Most system metrics, such as timeliness, can now be collected and stored automatically by the program itself, in this case LeaveWeb. There will always be friction between these interfaces, the larger the distance between the domains, the greater the amount of information loss.

If the process was reengineered and the stovepipes were reduced, the new process might look like this:

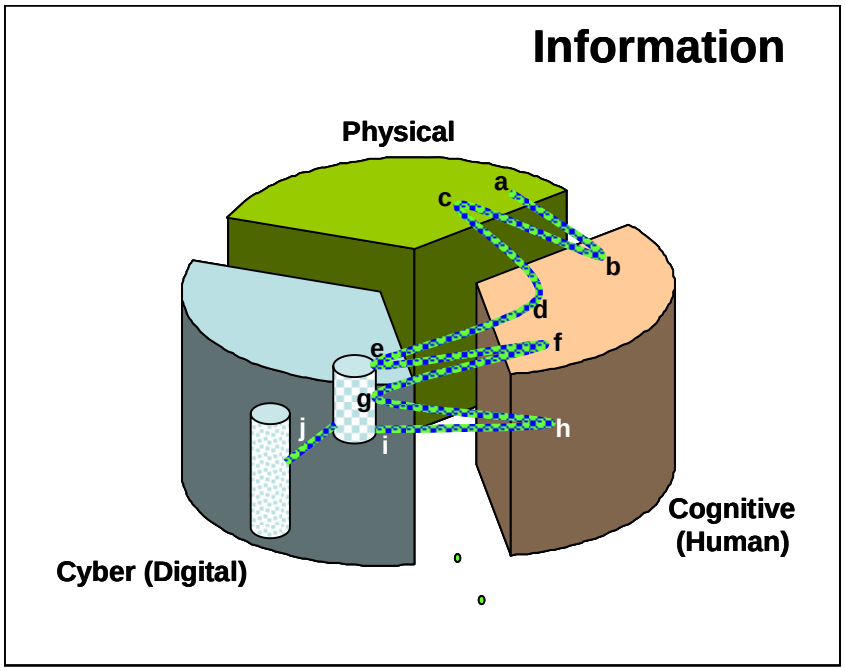

Figure 7. Reengineered Leave Process

a. A friend invites you on vacation
b. You determine if you want to go
c. You talk to your boss to determine if you can have the time away from work
d. Leave is approved, begin paperwork
e. Access LeaveWeb determine if you have leave and submit request
f. Supervisor approves leave
g. Updates in LeaveWeb
h. Orderly Room validates leave
i. Updates in LeaveWeb
j. Pay system automatically updated

Notice there are less steps in the process and less information lost (represented again by the single green dot).

The leave process also highlights one of the most difficult aspects of leveraging cyberspace to enable the reengineering of our processes is the preponderance of existing partially automated systems. We have enormous amounts of data and information stored away in stove-piped systems, databases and spreadsheets. Many well intentioned people of the Air Force have spent over a decade automating the portion of the process that they are directly in control of at their level. Unfortunately, this has un-intentionally created many system stovepipes that must now be broken down and integrated at a higher level. Only the USAF leadership can make this happen and even then it will be difficult.

As technology evolved, different organizations within the Air Force created systems that did not interface with one another. Additionally many did support the larger overall business process of the AF, only their specific piece the overall mission. We have even established unique doctrine and Air Force Specialty Codes (AFSCs) to maintain the different systems. Aircraft maintainers are stewards of Link 16, space operators control MILSATCOM systems over which Link 16 data passes, and communications officers

install and operate computers on which Link 16 data is compiled. This is graphically represented in Figure 9:

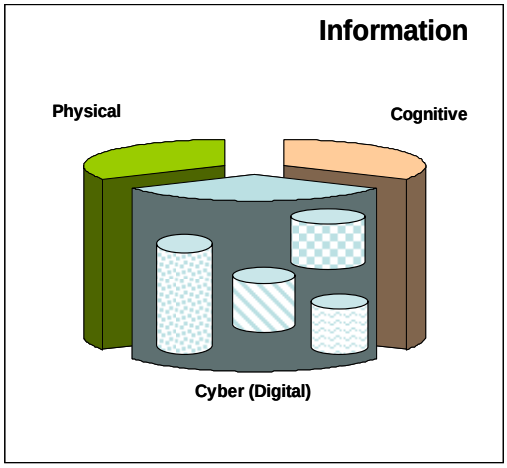

Figure 8. Cyberspace Stovepipes

Each stovepipe may look different, it is still cyberspace. For example, two well known stove pipes are the NIPRNET and Link 16 (a communications system used by military aircraft). Both systems exist in cyberspace, but they look very different, are governed by different doctrine and have different Air Force Specialty Codes (AFSCs) that maintain the systems.

While this type of configuration occurred due to the natural evolution of cyberspace, it is the causing difficulty when trying to interface those systems with other systems in cyberspace. To fully appreciate and understand the magnitude of the problem, one only has to look at the resources required in a Combined Air Operations Center (CAOC) and the multitude of screens on the walls because the common operating pictures can not be integrated.

The AF is certainly not alone in this; it is a problem that is plaguing many companies right now. Millions of dollars are being spent to put content online, but in

many cases it is not organized, so people struggle to find the information they need. While many organizations recognize the problem, these large scale efforts rarely succeed (Roberts-Witt, 2000, p. 2). As we continue to become more dependent on cyberspace, the cost of having systems that do not interface with each other will increase.

"In recent years, GAO has laid blame on some agencies' faulty management of IT contractors and said poor leadership and planning at DOD led to a stove-piped supply chain system that left soldiers in Iraq short of vehicles, tires, Meals Ready-to-Eat and even paychecks" (Essex, 2006). Recognizing these stovepipes and their associated affects on our business process is the first step in created more success like LeaveWeb and avoiding more failures that cross the functional communities.

Organization of the stored digital information is an increasing problem that is rapidly outpacing the problems of collection and transportation of the information. While we can store as much information as we want, we must avoid "Data Smog" because "the issue isn't so much acquiring the information in the first place, but remembering just where it was left" (Roberts-Witt, 2000, p. 1). Our data storage capability increases daily with each new computer connected to a network, consequently finding a way to store the information so that it is accessible and useable to all who need it is increasingly becoming a problem. "Knowledge by themselves are sterile. They become productive only if welded together into a single, unified knowledge" (Drucker, 1994, p. 50). In order to make our information and knowledge valuable to the war fighters, we need to make sure we can integrate it so we can get the right information to the right warfighter at the right time.

Cyberspace is rapidly becoming more than just a set of interconnected computer systems, therefore we need to approach them differently. If you pick up a book on Enterprise Architecture (EA), BPR, Lean, Strategic Information Management, Knowledge Management, or Network Centric Warfare (NCW) there is one clear message. We have to tie technology to our business processes, not vice versa. We must begin to take a high level systematic approach to breaking down these cyberspace stovepipes and reengineering our processes if we truly want to Fly, Fight *and win* in cyberspace.

IV. Cyberspace Capabilities and Mission Areas

We now have the foundation to discuss cyberspace capabilities and mission areas. As with the previous sections, we need to establish a common language that can be universally used so that we can leverage the capabilities, irrespective of platform or stovepipe, to achieve the desired effect of exploiting the adversaries while defending our portion of cyberspace. Technology will continue to evolve, so we must agree on some basic terminology that can also remain constant and still apply to the new technology. We can not define this is terms of the tools that are in use today, because what we can do today and what we can do tomorrow both in and through cyberspace and the tools used to accomplish that will change.

Unlike conventional warfare, it is difficult to tell what capabilities the enemy has (CyberWar!, 2003) In this invisible world, where information is the key, how do you know what information the other side has; do they have your passwords and you just

don't know it yet? And what does that mean if they do have your passwords if you can still trust and use your system?

Capabilities

There a two basic types of attacks in cyberspace you can attack the physical components (i.e. drop a bomb on a major hub of information) or you can attack the information contained in or transitioning the system. Physical attacks of the system are not new concepts with cyberspace; our critical information nodes have always been a target for kinetic or physical attacks. From the physical attack perspective we have the same vulnerabilities today as when we used the Pony Express; if we physically disable or block the components that carry the message, it will probably not get through unless the sender finds an alternate delivery path to send it. Consequently it will not be extensively covered in this paper. Attacking the information contained in or transitioning through the system is also not an inherently new concept, from the perspective that we have always had the problem of ensuring confidentiality and integrity of our information. However cyberspace does add additional dimensions because of the speed and amount of information that can be transferred so the problem will be discussed in further detail.

Significant research has been done to determine the types of attacks that can be affect information. Some believe that cyber attacks generally target availability, authentication, confidentiality and/or integrity (Kinkus, 2005). Joint Communications Systems Doctrine (JP 6-0), discuss seven criteria for information quality that might be attacked: accuracy, relevance, timeliness, completeness, brevity, usability and security. Additionally, it discusses the five aspects of information assurance confidentiality,

integrity, availability, authentication and non-repudiation. (JP 6-0, 2006) Are these actually *capabilities, tools,* or *effects?*

How do you *attack* authentication and non-repudiation? From a capability perspective is this really different than *attacking* accuracy of the information if the only thing that was modified is the source of the information? These terms are not capabilities within cyberspace but are effects. Fundamentally, the information was changed or modified, and the effect was losing the accuracy or the true identity of the message sender. In order to define the capabilities of cyberspace, we need to get back to the basics of what actions or combination of actions can be done in that domain.

There are three fundamental things you can do with information and all other aspects can be defined as combinations of these initial three. The primary capabilities include interception, modification, and denial.

The following model represents the capabilities and their combinations:

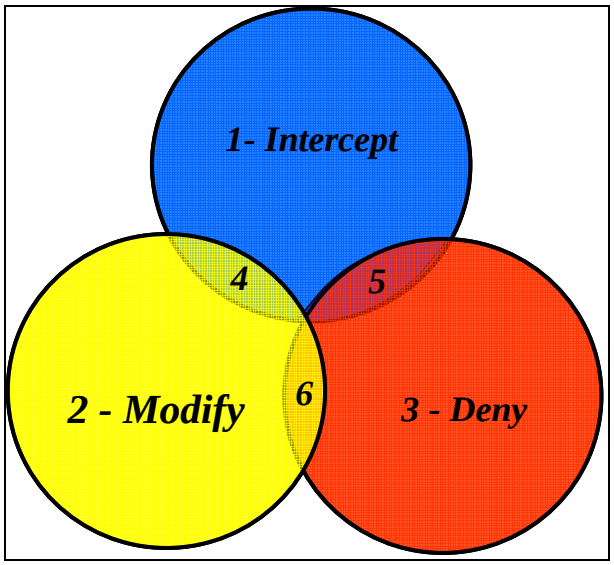

Figure 9. Cyberspace Capabilities

First, the primary capabilities are areas 1-3. Area 1, intercepting the information creates a copy of the information, but does not destroy or interfere with the transmission of the information. For example, one can intercept a telephone call without interrupting the telephone call or one can copy files without destroying the original files. Area 2, denying the information can either represent denying the enemy access to the information temporarily or destroying the information permanently. An example of this may be a denial of service attack, non-physical destruction such as deleting the files from a hard drive or even physical destruction. Area 3 – modify, represents changing the information or providing inaccurate information. An example of these capabilities includes gaining access to a computer system and changing the existing information or changing the information as it traverses cyberspace.

The secondary effects, areas 4 – 6, are actual combinations of the first effects. Capabilities in area 4 include intercepting the message, effectively creating an accurate copy, but instead of allowing the information to remain intact, it is modified as well. Area 5 represents intercepting the information, and simultaneously denying the information to the adversary. This is different than area 3 because in area 3 another copy is not created before it is denied. Area 6 represents the area where exploitation occurs. In this area the information resources are denied and instead used to provide information that the user does not want. A great example of this occurred in the movie "Independence Day" when the aliens used our satellite systems to synchronize their countdown sequence around the world.

Offensive Operations Example

In the offensive area, it is much easier for a commander to provide direction from this perspective. He/she basically asks three questions. Do we want the information? Do we want to modify or deceive the adversary? Do we want to deny the adversary's information? If so, effects can be specified as temporary or permanent. The answers to these questions will identify the correct region of the circle and then we can employ the modern tools that we have available. These tools can be anything in the inventory and do not have to be purely networking tools. For example, assume a commander wants to temporarily take out the integrated air defense system (IADS) shown in figure 10.

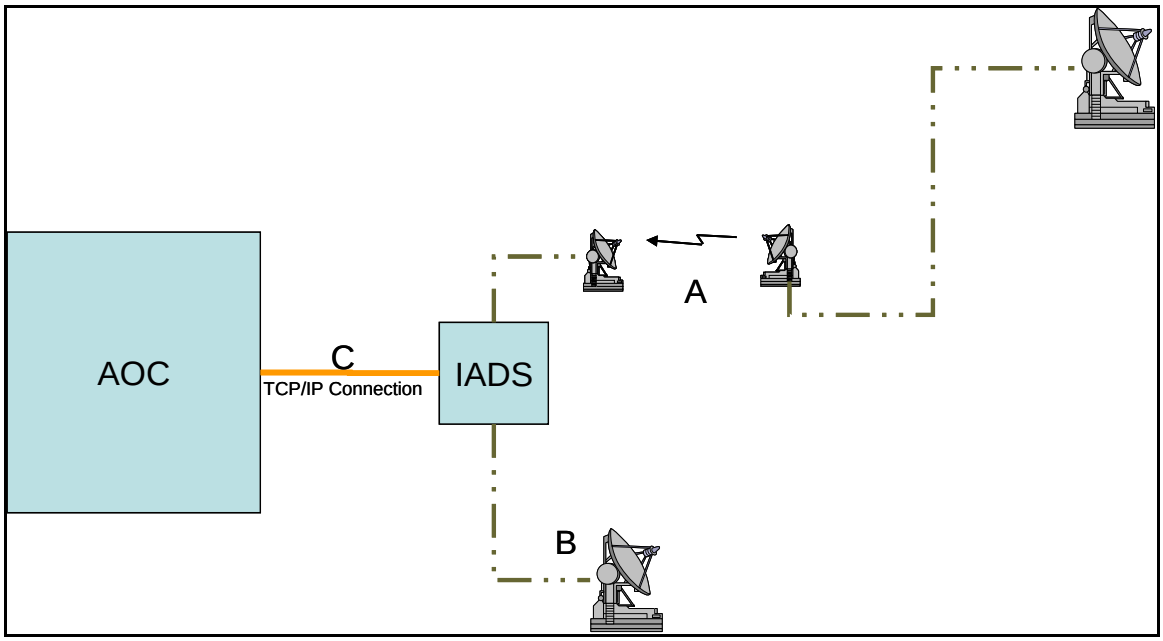

Figure 10. IADS

He/she wants to *temporarily deny* the use of the system, but does not want to modify or intercept any of the information from the IADS. In order for this IADS to work properly,

the radars must be able to send information back to the Air Operations Center (AOC). There are multiple options on *how* to temporarily deny the use of the IADS from this perspective

- Use electronic warfare (EW) to jam the radars
- A cyber attack to disable the connections at point C
- A cyber attack to disrupt the information within the IADS before it is sent over the network at point C
- Attack the IADS SCADA systems such as the power grid
- A combination, such as EW jamming at point A and a cyber attack at point B

The ultimate decision would depend on the capabilities and availability of the tools in the theater at the time of the request.

Currently, the EW communities governed by AF/A3, the intelligence communities governed by AF/A2 and the communications communities governed by AF/A6 do not necessarily speak the same language and they certainly do not belong to the same organization consequently these barriers may make it difficult to implement an efficient and effective combination, leaving the command with limited options.

Defensive Operations Example

On the defensive side it is also important to know what is happening to the information to enable better damage prevention and assessment. If an adversary launches a denial of service (DOS) attack the user would not be able to access information, but generally existing data does not get directly damaged. However, in the case of a web-based retail company, the damage could be catastrophic if no one can access the company's website during a busy shopping time and therefore the company loses sales. In the case of a website such as the Air Force Virtual MPF, a DOS attack might cause

frustration to customers. It will cost the Air Force in morale and lost productivity of those members while the problem gets solved, but it probably won't put the Air Force out of business. If, however, a DOS attack blocked our ability to transmit and receive the Air Tasking Order for the day or conduct rescue operations, we would not be able to complete our mission, and lives could be lost if we don't realize that we are under that type of attack and reroute our information.

In the case of intercepted information where it does not damage the information, only copies it. We would of course still have access to it; however, if hackers target the authentication portion of a system, they will attempt to gain access pretending to be someone else. Once they have established a fake identity, hackers can get into our internal systems and cause significantly more damage than they could have on the outside. This could be considered an enabler of the other types of attacks because it allows a "bad" user full access of the system to damage it directly at a later time. So if we know there is hacker activity present, it is important to understand what capability they are employing so we can properly assess current damage and future vulnerabilities.

Other attacks aimed at interception information can be equally dangerous because nothing is initially damaged, it can have grave effects at a later date. For example, if classified information was stolen about an upcoming operation, lives could be lost as a result. Stealing intellectual property could be the most undervalued and misunderstood attacks. In the area of trade secrets or classified information, what if it is copied? Technically the information is still there, so we can use it (unlike a car that we could not use if it were stolen), but the theft could cause us to lose competitive advantage over the

adversary. Trade secrets can be stolen in the corporate world, forcing the company out of business at some point later in time.

Modification of the data can be very damaging, and sometimes very difficult to find. For example, what if the malicious code just updates part of the data to indicate that the inventory on hand is zero? A commercial company could lose money in lost sales and then have to spend additional resources to re-accomplish the inventory to get the information corrected. In the military environment, this could impact our supply chain, crippling a unit because they don't have necessary resources to complete the mission. This is also very hard to find and it can lead to distrust of the information because the company does not know what has been modified and what has not. Consequently, the time to return the data to its original state is enormous because *everything* must be checked.

Cyberspace as a Mission

"The results of an army are not maneuvers and promotions for generals; they are deterring a war or winning it" (Drucker, 1994, p. 55). Fundamentally, we want to bend the enemy to our will, in the most humane way possible with the least amount of casualties on both sides. We, as a service, have a responsibility to protect our nation's interests and way of life. In cyberspace, system boundaries are sometimes difficult to define (i.e. web based applications) consequently we can not protect them in the conventional way. The National Strategy to Secure Cyberspace also recognizes that this must be a partnership between the private sector and the government. The strategy

identifies three main objectives: “Prevent cyber attacks against America’s critical infrastructures; reduce national vulnerability to cyber attacks; and minimize damage and recovery time from cyber attacks that do occur.” (White House, 2006, p. 16)

Adding cyberspace to our mission statement is a logical step based on the evolution of technology. “No organization in the fifty years since World War II has changed more than the military, even though uniforms and titles of rank have remain the same” (Drucker, 1994, p. 59). Cyberspace is a relatively new medium that had to evolve to include its current capabilities before we could define it as a mission area. Through this evolution unique doctrine and cultures have been developed both in the military and the private sector making it difficult to define but important to recognize. Looking at this new digital environment from an information flow perspective aids in identifying where we can reorganize and concentrate our efforts.

We must define our cyberspace mission broadly based on the capabilities of cyberspace not the tools and effects generated by cyberspace. When we first became a service, the focus was strategic bombing. However as airplanes and airpower evolved fighters, bombers and mobility missions combined to define the air superiority we enjoy today. Organizations should “position themselves strategically based on their unique, valuable, and inimitable resources and capabilities rather than the products and services derived from those capabilities” (Drucker, 1994, p. 127). When defining our mission statement for cyberspace, we want to look broadly across all dimensions of what is possible.

“Forces are at risk without complete, secure, assured, and timely information” (NETWARCOM, 2006). We use the systems within cyberspace to pass this information

quickly across the globe and figure 11 shows the areas that can be attacked and need to be defended.

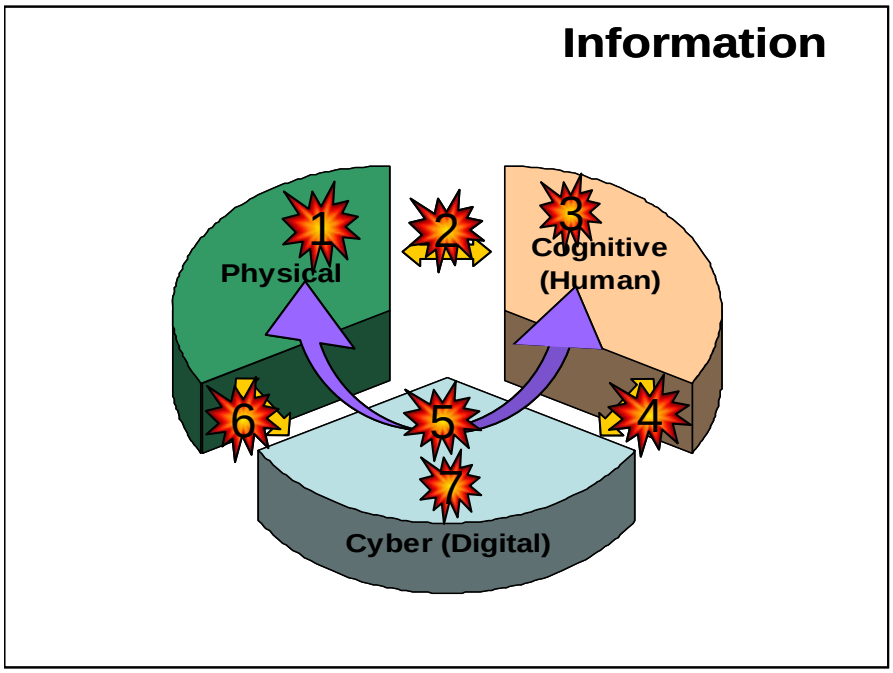

Figure 11. Areas of Vulnerability

The areas above are defined as follows:

1. **Information about the physical environment**: This information changes when the physical domain changes, i.e. deception, hiding tanks under camouflage netting.
2. **Interface between physical and cognitive domains**. This information is basically defined in the term of our 5 senses (hearing, touch, smell, sight, taste). And example of this information bad HUMIT to mislead, or keeping them from interacting with the physical world (i.e. kidnapping), using the incorrect language (i.e. a foreign language)

3. **The cognitive environment:** Affecting the health and wellbeing of the actual people.
4. **Interfaces between cognitive and cyber domains:** Affecting the transfer of information in/out of cyberspace to the human domain (i.e. the screens, keyboards, etc)
5. **Information transitioning through cyberspace that affects the physical world:** Taking control of systems that use cyberspace to control provide the link to control the physical world (i.e. UAV and SCADA systems)
6. **Interaction between the cyber and the physical Domain:** Affecting the transfer of information in/out of cyberspace to the physical domain, for example intelligence reconnaissance systems
7. **Information repositories/Processes in the Cyber Domain:** Affecting the information stores and transmit systems in cyberspace. This can be attacks on servers or other information stores as well as the pieces that provide the connectivity.

All areas are areas of information, however attacking areas 1 – 3 are not related to cyberspace, simply information. Areas 4-7 relate directly to cyberspace and therefore should be the areas that future cyber organizations focus on. We have to have unity of command to remove the seams in our processes so that we limit the amount of information that is lost or vulnerable as it crosses between the domains of information. Areas 6 address the interfaces between cyberspace and physical worlds. The functions that currently reside in Area 6 include intelligence and EW applications. Area 4 tends to

be the human factors area, and presenting the information in a usable format. Although not defined as a community, the sole purpose of all the screens in the CAOC are dedicated to this interface, why not combine the efforts? Area 5 and 7 include all the systems within cyberspace and transiting though it. Network Centric Warfare is not just about connecting weapon systems together on a communications network. It is about utilizing the connectivity of the network to transform operations and doctrine (Logan, 2006). As we increase area 5, we need to remember "the complexity of the warfighter's mission increases as each new weapon system or technology is added to the battle space." (Klausner, 2002, p. 1) Especially if we are not eliminating some legacy systems in the process.

One aspect of cyberspace that is limited is the radio frequency (RF) spectrum. This limitation is a function of current technical capability as well as national and international policy. This spectrum is rapidly being allocated to wireless applications and increased bandwidth requirements such as UAVs. Radio frequency management in other countries is likely to make this a very limiting factor in the future. "[B]andwidth allocation and management are now as operationally important as airspace control and the allocation of tanker, jamming, and defense-suppression assets" (Klausner, 2002, p. 5).

The Tenets of Air, Space and Cyberspace

Finally, the air and space power tenets were studied in depth to see if the current tenets apply to cyberspace and to see if any additional tenets should be added with the addition of cyberspace as a mission statement. Air Force Basic Doctrine (AFDD 1),

describes seven tenets of air and space power: centralized control and decentralized execution, flexibility and versatility, synergistic effects, persistence, concentration, priority, and balance. After studying each tenet, all of the current air and space tenets apply to cyberspace.

Does cyberspace add anything new? There are significant amounts of principals, tenets and capabilities referenced in joint and AF doctrine. Unfortunately, because of the different community stovepipes the capabilities were often defined in terms of the platforms or tools that used them, not in the capability itself. Additionally, many documents referred to the same basic principals but used different words to describe them such as *flexibility, agility* and *versatility*. All of which could mean basically the same thing with minor nuances. However, three new tenets were recommended as additions to the current tenets *responsiveness*, *reliability*, and *global perspective*. (Roth, 2006)

Responsiveness and reliability address the critical items that must be in place to be able to effectively utilize the systems in the cyberspace domain. These tenets address the concepts of timeliness, on-demand access, accuracy, security, confidentiality, integrity, availability, authentication, and non-repudiation.

Global Perspective addresses the power that cyberspace enables. It addresses the Network Centric Warfare concepts of improved information sharing, shared situational awareness and informed decision making. Without cyberspace, having a real time global perspective of the environment, such as the common operating pictures in the CAOC, would not be possible.

V. Conclusion

We cannot go back to a time before cyberspace as a nation. Therefore we must take deliberate steps to harness the power and capabilities cyberspace in order to ensure our nation is safe. Cyberspace evolved and with it many unique stove piped systems, processes and language. The first step in brining these systems together is establishing a common language to discuss cyberspace and the capabilities within it. We must get back to the basics of what cyberspace is, why it is so unique and important, and how we can utilize cyberspace capabilities in our missions. Our dependence on this digital environment, known as cyberspace, will continue to grow because of the capabilities offered by new technology. However, these technology advances have the potential to redefine how we define cyberspace if we do not remember the fundamental principals of why we have it – to collected, store, process, and transmit information – and what we can do with it. Cyberspace may be a potentially boundless environment enabling our real time global perspective, but our budgets and the amount of information we can humanly process are not. As our dependence increases and our budgets shrink we need to effectively manage our cyberspace assets and capabilities to ensure we can Fly, Flight *and win* in Cyberspace!

Bibliography

1. Air Force Doctrine Document (AFDD) 1, Air Force Basic Doctrine, 2003, 10 May 06 [On-line]. Available: http://www.dtic.mil/doctrine/jel/service_pubs/afdd1.pdf

2. Air Force Doctrine Document (AFDD) 2-5, Information Operations, 2005, 10 May 06 [On-line]. Available: http://www.dtic.mil/doctrine/jel/service_pubs/afd2_5.pdf

3. Air Force Doctrine Document (AFDD) 2-5.1, Electronic Warfare, 2002, 10 May 06 [On-line]. Available: http://www.dtic.mil/doctrine/jel/service_pubs/afd2_5_1.pdf

4. Alberts, David S., Garstka, John J., Stein, Frederick, P. *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition, 1999, CCRP Publication Series

5. Alberts, David S., Garstka, John J., Network Centric Operations Conceptual Framework, version 2.0, 2004, Evidence Based Research, Inc

6. Cyber War! Prod. Michael Kirk. Public Broadcasting System, 24 Apr 2003

7. Dictionary.com *On-Line*, 10 Apr 06 [On-line] Available: http://dictionary.reference.com/search?q=cyberspace

8. Drucker, Peter F. *Post-Capitalist Society*. New York: HarperCollins Publishers, 1994. (5)

9. Essex, David, Agencies chip away at BSMs, Government Computer News 16 May 06 [On-line]. Available: http://www.gcn.com/print/25_12/40758-1.html

10. Kinkus, Jane F. *Computer Security*, [On-line] 26 Oct 05 Available: http://www.istl.org/02-fall/internet.html (26 Oct 05).

11. Klausner, Kurt A. (2002), Command and Control of Air and Space Forces Requires Significant Attention to Bandwidth, *Air & Space Power Journal*, Winter 2002 [On-Line] Available: http://www.airpower.maxwell.af.mil/airchronicles/apj/apj02/win02/klausner.html

12. Halbert, T. & Ingulli, E. (2005). *Cyber Ethics* (2nd ED). Eagan, MN: Thomson-West.

13. Hammer, Michael. & Champy, James (2003). *Reengineering the Corporation: A Manifesto For Business Revolution*. New York, NY: Harper Collins Publishers, Inc.

14. Heminger, Alan and others, "Analysis of Air Force Materiel Command E-Business Initiatives." Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, Apr 2006.

15. Heminger, Alan. Class Lecture, IMGT 684, Strategic Information Management, School of Management, Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, Jan 2006.

16. Joint Publication (JP) 1-02, DOD Dictionary of Military and Associated Terms, 12 April 2001 [On-line] Available: http://www.dtic.mil/doctrine/jpreferencepubs.htm

17. Joint Publication (JP) 2-01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battle space, 24 May 2000 [On-line] Available: http://www.dtic.mil/doctrine/jpintelligenceseriespubs.htm

18. Joint Publication (JP) 6, Joint Communications Systems, 2006, [On-line] Available: http://www.dtic.mil/doctrine/jel/new_pubs/jp6_0.pdf

19. Jones, Daniel T. & Womack, James P, 2003, *Lean Thinking: Banish Waste and Create Wealth In Your Corporation*. New York, NY: Free Press.

20. Logan, Bradley C., Boeing - Technical Reference Model for Network-Centric Operations. 1 May 06 [On-line] Available: http://www.stsc.hill.af.mil/CrossTalk/2003/08/0308logan.html

21. Merriam-Webster On-Line Dictionary, 17 May 06 [On-line]. Available: http://www.m-w.com/

22. Navy's Central Operational Authority for Network, Information Operations, and FORCEnet, https://ekm.netwarcom.navy.mil/netwarcom/nnwc-nipr/index.htm, 8 May 06.

23. Negroponte, Nicholas, *Being Digital.* New York: Alfred A. Knopf, Inc 1995

24. Princeton. WordNet Search, 17 May 06 [On-line] Available: wordnet.princeton.edu/perl/webwn

25. Roberts-Witt, Sarah L., Practical Taxonomies, Destination KM.Com, December 11, 2000, http://www.kmmag.com/print/default.asp?ArticleID=684, 4/21/06 (7)

26. Roth, Kristina & Woolley, Pamela "Tenets of Cyberspace" Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, May 2006.

27. Stone, Brad, Factory of the Future article, Newsweek. 22 Nov 2004.

28. University of Arizona. On-Line Library, 17 Apr 06 [On-line] Available: www.library.arizona.edu/rio/glossary.htm

29. University of New Orleans. On-Line Distance Learning Glossary, 17 May 06 [On-line] Available: alt.uno.edu/glossary.html

30. Webopedia, On-Line Dictionary, 1 May 06 [On-line] Available: http://www.webopedia.com

31. White House, The National Strategy to Secure Cyberspace, Washington: Feb 2003 1 May 06 [On-line] Available: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

32. Zack, Michael H. Developing a Knowledge Strategy, California Management Review, Spring 1999; 41, 3, page 125-145…. Also quoted within a quote: R.M. Grant, "Prospering in Dynamically Competitive Environments……"

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
13-06-2006	**Graduate Research Project**	May 2005 – June 2006

4. TITLE AND SUBTITLE

Defining Cyberspace as a United States Air Force Mission

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Woolley, Pamela, Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/IC4/ENG/06-09

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AF/XP
ATTN: Dr. Lani Kass
1670 Air Force Pentagon, Room 4D544
Washington, DC 20330-1070
Comm: (703) 697-2807 Email: lani.kass@pentagon.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this research was to provide a common framework and language for the definition of cyberspace. Specifically this project looked into three key areas what cyberspace is, why it is unique and important, and the capabilities and mission areas. An extensive literature review was completed. The research indicated that the fundamental problem of defining cyberspace evolved as cyberspace evolved within each community in the Air Force.

The culmination of this effect was an encompassing definition as well as a set of models to graphically depict cyberspace and the interactions with the other information domains.

15. SUBJECT TERMS

Cyberspace

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			**Robert Mills, PhD (ENG)**
U	**U**	**U**	**UU**	46	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565 ext 4527; email: Robert.mills@afit.edu

Standard Form 298 (Rev: 8-98)
Prescribed by ANSI Std. Z39-18